University of Oregon

COMPUTING NEWS

Fall 2004

Welcome back to campus, and to computing and networking at the University of Oregon!

IN THIS ISSUE…

Get Your Free Duckware 2004 and

The latest Duckware and Windows Security CDs are here! Bring your UO picture ID to any one of the distribution sites on campus and pick up a copy

It's fall, and once again it's time to get the latest edition of the Duckware CD. If you're a UO Windows user, you'll also need to pick up a copy of the 2004 Windows Security CD and a Norton Antivirus 2004 CD.

Duckware 2004 is a collection of the latest antiviral and network software designed to help you with computing at the UO. Duckware CDs contain step-by-step instructions for using the university's modem pool, wireless network, and VPN connections. They're available in both Mac and PC versions and are free to currently enrolled UO students, faculty, and staff.

Windows Users. This year's Windows edition includes the anti-spyware tool Spybot 1.3 and web browsers Firefox, Mozilla, and Netscape. Norton Antivirus 2004 is available on a separate CD, which is free to UO students, faculty, and staff.

Windows Security CD: UO Windows users will also need to pick up a copy of the 2004 Windows Security CD, which contains vital antiviral updates and system patches specific to Windows machines. ***Be sure to run this security CD BEFORE you connect to the campus network!!***

Mac Users. The Mac Duckware CD contains Norton AntiVirus 9.0, Fugu 1.1, and web browsers Firefox, Mozilla, and Netscape.

Because the Mac operating system is unaffected by viruses currently in the wild, Mac users do not need a supplemental security CD.

System Requirements

PC users: To use Duckware 2004, you'll need Windows 98, ME, 2000, or XP.

Mac users: The Macintosh version is compatible with Mac OS X.

Where to Get Your CDs

Campus locations. UO students, faculty, and staff may pick up a copy of the Duckware 2004 CD and Windows Security CD at the following campus locations:

- Microcomputer Support Center (151 McKenzie Hall)
- Documents Room Library (175 McKenzie Hall)
- CC-McKenzie Lab (101 McKenzie Hall)
- CC-EMU Microcomputing Lab (22 EMU)
- CC-Klamath Lab (B13 Klamath Hall)
- CC-Millrace Lab (113 Millrace I)

- continued on p. 3

UNIVERSITY OF OREGON

COMPUTING CENTER

COMPUTING NEWS

VOL. 19 #4

Computing News is published quarterly by the User Services and Network Applications staff of the Computing Center.

Contact: Joyce Winslow
jwins@uoregon.edu

Photography: Dave Ragsdale
dave@uoregon.edu

Joe St Sauver, Ph.D.
Director, User Services
and Network Applications
joe@uoregon.edu

Website:
http://cc.uoregon.edu/cnews/

Got Extras?

If your campus department receives surplus copies of *Computing News*, you may return them to the UO Computing Center for redistribution.

Manage Your UO Computing Account Online

- Read your email: **http://email.uoregon.edu/**
- Change your password: **https://password.uoregon.edu/**
- Reset your password: **https://password.uoregon.edu/authorize/**
- Forward mail: **http://password.uoregon.edu/forward/**
- Remove mail forwarding: **http://password.uoregon.edu/noforward/**
- Check your disk quota: **https://password.uoregon.edu/quota/**
- Disable/re-enable spam filtering: **https://password.uoregon.edu/allowspam/**

One-stop shopping for account management: You'll also find links to all of these account functions on Microcomputer Services' Account Management web page at **http://micro.uoregon.edu/account/manage.html**

Windows Security CDs

- AAA (280 Lawrence Hall)
- Knight Library Information Technology Center (second floor, Knight Library)
- Science Library Information Technology Center (lower level, Onyx Bridge Building)

Campus housing distribution. Students living in campus housing can get Duckware at Residence Hall and Family Housing area desks in the University Inn, Carson, Spencer View, Westmoreland, and in the ResNet office (101 Douglass Hall, Walton Complex).

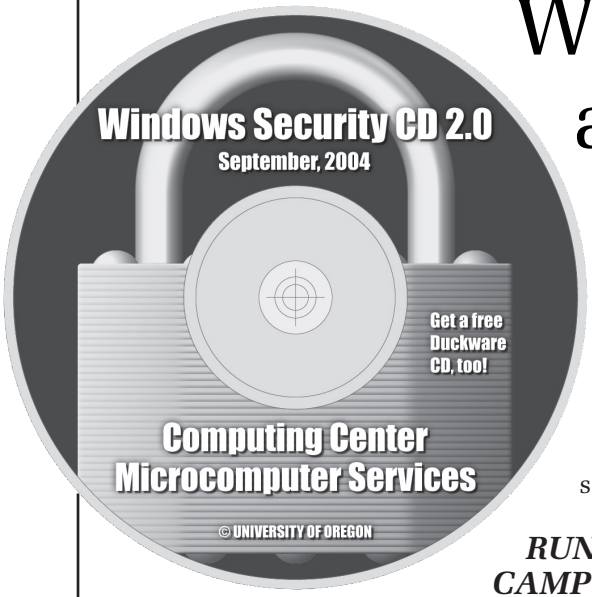
Reuse and Recycling

If you decide you no longer want your copy of Duckware 2004, please don't throw it away! We'll gladly take it back and give it to someone else. Just drop it off at the Microcomputer Support Center, or mail it via campus mail to "Microcomputer Services, 151 McKenzie Hall."

Help

For additional Duckware help or information, contact the Microcomputer Support Center (**346-4412**, *microhelp@lists.uoregon.edu*).

You can also drop by 151 McKenzie Hall weekdays from 9 A.M. to 5 P.M., or visit their website at **http://micro.uoregon.edu/**



What You Need to Know about the 2004 Windows Security CD

Like Duckware, the Windows Security CD automatically plays when inserted into your computer's CD-ROM drive. The program on the Security CD checks to see if your system is already infected, and tries to remove any exploits. It applies the appropriate patch for Windows 2000 or XP systems (Windows ME, 98, and 95, and all Mac OS systems are not affected). As a final measure, virus definitions are updated and a scan is invoked.

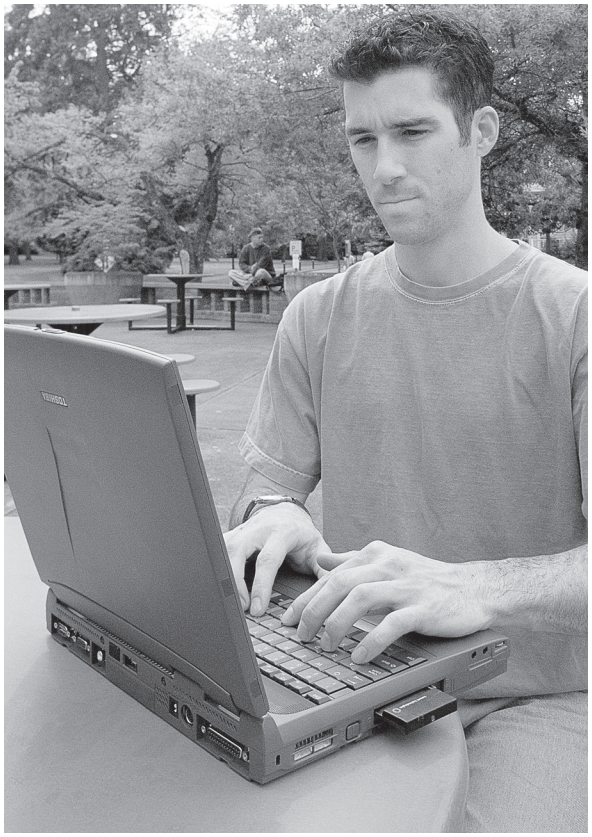
RUN THE SECURITY CD BEFORE CONNECTING TO THE CAMPUS NETWORK! The infection rate of current worms is so fast, you will not have time to download the updates from Microsoft's Windows Update site before becoming contaminated. *For this reason, you must use the security CD* ***before*** *connecting to UOnet.* ***Ethernet users should physically unplug their Ethernet cable, run the security CD, reboot, and plug the cable back in only after the CD's protective cycle is complete.***

Keep a record of any error messages. Users need to pay attention to any error messages Norton Antivirus may display, and write them down.

Troubleshooting help. It is possible for Norton to detect a worm, virus, or trojan that it cannot eradicate. If that occurs, Norton will indicate the virus name, and which files it could not delete. This information may be necessary for later troubleshooting.

If you run into a problem you can't resolve, call Microcomputer Services at **346-4412**.

New to Campus? Don't Know Where Here's How to Begin Using Your UO



If your mind is reeling with questions about computing at the UO, here are some tips to help you get started…

When you register for classes, we automatically generate a computing account for you that consists of a username and password. Your computing account is used for email, dialin access, VPN, wireless, and Blackboard.

If for some reason you don't have a UO computing account, pick up a copy of the handout, "How to Get a Computing Account," available in the Documents Room Library (175 McKenzie Hall), or online at **http://cc.uoregon.edu/policy/get_account.html**

How Do I Start Using Email?

There are three ways to get your account information:

- via DuckWeb (**http://duckweb.uoregon.edu/**)
- in person, by going to the Microcomputer Support Center (151 McKenzie Hall) and presenting your photo ID.
- by accessing the AUTHORIZE program from your web browser (**https://password.uoregon.edu/authorize/**)

What About Passwords?

You should pick your own password instead of simply using the one that's generated for you. Here's how:

1. Open your network browser (e.g., Netscape, Mozilla) and go to **https://password.uoregon.edu/**
2. **If you know your old password**, enter your username and old password in the spaces provided. Type in your new password and enter it again for verification.
3. **If you don't know your old password**, you'll need to know your student ID number and PAC code. Go to **https://password.uoregon.edu/authorize/** Enter your student ID and PAC code in the spaces provided, and follow the instructions for creating a new password.

Password security: Passwords should be 6 to 14 characters long and must be very secure. We recommend choosing a password that's a mixture of mixed-case letters and numbers. Dictionary words and any part of your name are not allowed. For more detailed information on password policy, see **http://cc.uoregon.edu/policy/passwd_policy.html**

Note that you will need to change your password every six months or so.

What About Off-Campus Connections?

Your computing account username and password are the same ones you'll use for accessing UOnet from off-campus, whether you're dialing in with a traditional modem or connecting via the UO's VPN service through commercial DSL or cable modem service.

Traditional modem. If you're dialing in via modem, you must type in your full username address to dial in, including your account's hostname (for example, **jersmith@gladstone.uoregon.edu** or **jersmith@darkwing.uoregon.edu**) The modem number for accessing UOnet, the campus network, is **225-2200**.

Note: *Your modem access is for casual use—no more than a few hours a day on average. If you need dedicated or near-dedicated network access, you'll want to contact a commercial Internet Service Provider. You should also be aware that we have recently installed security filters that inhibit the use of Microsoft networking from dialup modems. If you really need to use Microsoft networking, the workaround is to install and run the VPN software included on Duckware.*

---

to Start?
Computing Account

High-speed DSL or cable modem connections. If you have an account with a commercial Internet Service Provider, you may want to log in to your UO account using the UO's Virtual Private Network (VPN) software. VPN allows you to securely access resources normally restricted to on-campus use—such as the UO's software distribution sites or restricted library databases. If you do *not* use VPN, for security purposes we recommend using end-to-end encryption tools such as the SSL included in your web browser, or SSH for shell and file transfer (for more information on SSL and SSH, visit the Micro Services security site at **http://micro.uoregon.edu/security/**)

For a good overview of VPN, see **http://micro.uoregon.edu/getconnected/vpn_overview.html** Instructions for connecting to VPN are available at **http://micro.uoregon.edu/getconnected/**

What About Wireless?

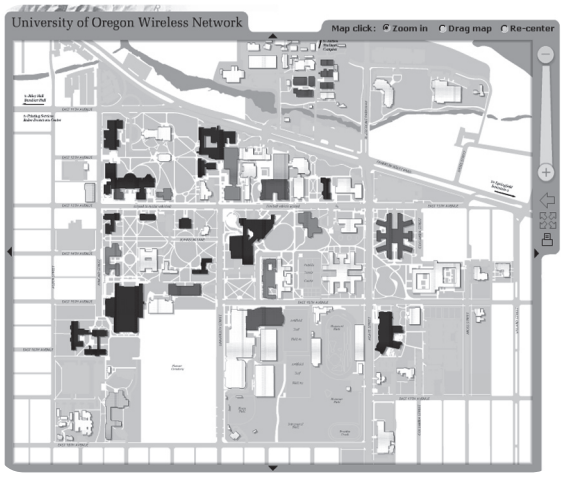
You can also access UOnet in several public areas on campus via an 802.11a/b/g card in your laptop computer. Your device must have appropriate drivers for your wireless card and a web browser that supports SSL encryption. To connect to UOnet, you will need to authenticate with your Darkwing or Gladstone account username and password.

Security Note: Wireless users are especially vulnerable to electronic eavesdroppers. If you're using a wireless device and an application that lacks end-to-end encryption, you may wish to use the VPN software for added protection. For more information on campus wireless and current areas of coverage, including detailed set-up instructions, see **http://micro.uoregon.edu/wireless/**

What About Campus Housing Connections?

Every room in every UO residence hall has an ethernet connection (ResNet). Your computer will need an ethernet card. If you are a UO student living in the Residence Halls, University Housing can not only sell you an ethernet card for your computer, but install it and set it up free of charge. For more information about ResNet and details about purchasing an ethernet card, see **http://housing.uoregon.edu/resnet/**

Looking for a current map of wireless coverage on campus?



Go to:

http://geography.uoregon.edu/infographics/wireless/

This dynamic online map shows you the big picture. You can zoom in and out, scroll to a specific spot on campus, or search by entering a building name. The map is updated periodically as new wireless coverage is added.

FREE WORKSHOPS:
THE INFORMATION TECHNOLOGY CURRICULUM

See the fall schedule of classes at
http://libweb.uoregon.edu/it/

UO Computing Labs, Help Desk Are

Need help getting your new student computing account information? Help Desk consultants in 151 McKenzie can assist you with this, as well as a wide range of other computing questions and problems. The Help Desk is also one place you can pick up your copy of Duckware and the Windows Security CD.

Consulting Help

Microcomputer Services consultants are on hand every weekday from 9 a.m. to 5 p.m. at the Help Desk in 151 McKenzie Hall to help you with almost any question you may have about your Mac or PC, including how to:

- connect to the Internet from home or on campus
- get your new student computing account information
- deal with password problems
- transfer files
- eradicate viruses and protect yourself from future infection
- install and configure system software and troubleshoot problems
- repair damaged files and disks
- access public domain software

Student Accounts. Microcomputer Services staff can help with student accounts and password changes. New students can also obtain their account information via DuckWeb (**http://duckweb.uoregon.edu/**) using their student ID number and PAC code.

For complete information about student accounts, see **http://micro.uoregon.edu/getconnected/** or pick up a copy of the handout "New Students: Get Online!" in 175 McKenzie (the Computing Center's Documents Room Library).

Complex Problems. For customers who encounter particularly complex or hard-to-diagnose problems, Microcomputer Services offers a machine check-in service that costs $80.00/hour, billed by the quarter hour. Typical problems requiring machine check-in include those that involve reinstallation of operating system software, diagnosis of corrupt data, virus removal, and resolution of particularly difficult hardware conflicts that manifest themselves in software. Visa and MasterCard are accepted.

Multimedia Facilities

Microcomputer Services also has public stations in 151 McKenzie for scanning, CD copying and burning, and digital video acquisitions. (As in all electronic copying activities, copyright restrictions must be observed.) These services are available to UO students, faculty, and staff. Current services include:

PC Station (Windows XP, 45GB disk, 256MB RAM, Firewire support, Plextor 8x20 SCSI CD-R, Viewsonic G790 19" monitor):

- scanning: OCR (Optical Character Recognition), regular, and slide
- CD-ROM creation and duplication
- video in and out
- direct VHS/S-VHS into MPEG-1 in real time
- direct VHS/S-VHS into MPEG-2 in real time
- Some editing features using Adobe Premiere and Photoshop
- ZIP (100MB) and JAZ (2GB) drives

At Your Service Throughout the Week

Mac Station (Mac OS X 10.2, dual 1 GHz processor, 512MB RAM, 75GB hard drive, CD-RW, DVD-R, Firewire support):

- scanning
- video in and out
- video editing with iMovie and Adobe Premiere
- CD-ROM creation and duplication
- DVD creation using iDVD
- some editing features using Adobe Photoshop
- ZIP (100MB) and JAZ (2GB) drives

The PC is outfitted with two 18.1 GB, high-speed SCSI hard drives to facilitate the capture of large video files. To speed the transfer of data over UOnet, both the PC and Mac machines have 100MB/sec Ethernet connections.

Each station has a two-hour time limit and is available on a first come, first served basis.

Storage media. You may purchase up to 5 CD-R disks at $2 each in 151 McKenzie Hall if you wish. If you need more, you'll want to purchase them before coming in. ZIP or JAZ cartridges are not available.

Help. Microcomputer Services staff is available to assist you with basic use and start-up questions. If you need in-depth training for such skills as how to create CD-ROMs, capture video, or edit images, you will probably want to take some classes first. For more information, contact Microcomputer Services at **(541) 346-4412** Monday through Friday, 9 A.M. to 5 P.M.

Instructional and Drop-in Computing Labs on Campus

Instructional labs. The Computing Center has four computing labs available for use by instructors. Windows labs are located in B26 Klamath and 101A McKenzie, and Macintosh labs in B13 Klamath and 113 Millrace. Each lab is equipped with 20 to 24 computers and a variety of software. New software this year includes Adobe Creative Suite CS, Director 2004, Dreamweaver 2004, Fireworks 2004, and Flash 2004.

Reserving a lab for instructional use. Instructional labs are generally reserved for classes and lab sessions several terms prior to the term needed; however, there are a few times that are still available for instructional use. If you are interested in reserving a lab, please contact Mary Bradley (*labhelp@darkwing.uoregon.edu*, **346-1737**).

Drop-in labs. Besides instructional space, the Computing Center also maintains drop-in labs. There are drop-in lab facilities at each of the instructional sites, plus a large drop-in lab located in the basement of the EMU:

CC-EMU Lab. 22 EMU (in the basement near the Recreation Center and Arcade). **346-1769**

Millrace I Lab.113 Millrace I. **346-0316**

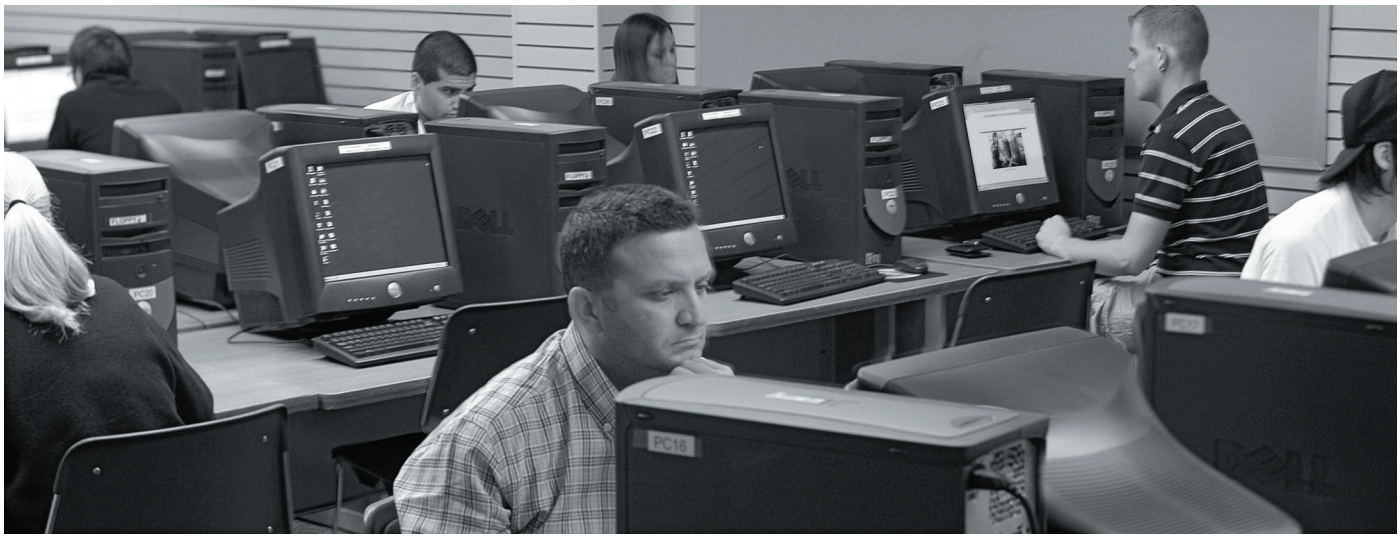
CC-Klamath Lab. In Klamath B13 and B26. **346-4781**

CC-McKenzie Lab. 101 McKenzie Hall (ground floor). **346-0787**

Other Campus Computing Labs:

Knight Library ITC - **346-1935**
Science Library ITC - **346-1331**
Social Science Instructional Lab - **346-2547**

For complete details about the software and services in all of these labs, as well as other computing labs on campus, see **http://cc.uoregon.edu/campuslabs.html**



*The CC-EMU drop-in lab in the basement of the EMU is a popular resource for students. Instructors may reserve some of the labs for class use each term. If you are interested in reserving a lab, please contact Mary Bradley (labhelp@darkwing.uoregon.edu, **346-1737**).*

Need Repair, Upgrades? Go to the E-Shop

If your laptop is on the blink, your printer's erratic, or if you simply need more cables or computer batteries, you can find what you need here on campus at the Computing Center's Electronics Shop (E-Shop).

Conveniently located on the ground floor of McKenzie Hall in Room 151, the nonprofit E-Shop offers extensive personal computer hardware support and repair services to UO students, faculty, and staff.

Apple Repair. The shop is a Level 1 Apple-authorized service center and can perform warranty, AppleCare, and out-of-warranty repairs on nearly all Mac models and peripherals.

PC Repair. The shop can perform non-warranty repairs on virtually all desktop and laptop models.

Upgrades. E-Shop technicians can help you determine the best and most cost-effective way to upgrade your machine. The shop keeps memory in stock for virtually all PC and Mac desktops and laptops.

Custom Systems (including backup solutions such as Firewire/USB and CD-RW drives or DVD superdrives). If you need a backup solution or a custom system configuration, such as a server with multiple SCSI controllers and mirrored disk drives, talk to the technicians. The shop may be able to build you a machine at considerable savings.

Parts. You'll find a wide selection of cables, hard drives, CD-RWs, adapters, and ethernet and USB hubs and switches at the shop. The shop stocks many PC parts, as well as ethernet cables and cables for printers and monitors, so you won't have to wait or travel far to get what you need.

You'll find an array of new parts and popular backup solutions at the E-Shop, some of which are pictured here. On the periphery, left to right: external CD-ROM burner (Firewire/USB), USB serial converter, laptop/desktop external HD case (Firewire/USB), 1GB bootable Flash "Jumbo Drive," high-speed hub and USB-to-Ethernet adapter.

Rates. Upgrades and out-of-warranty repairs are charged on a time-and-materials basis. The initial diagnostics fee is $40, and the current labor rate is $80/hour, billed by the quarter hour. As a convenience to customers, the shop now accepts Visa and MasterCard.

Hours and Policies. The shop is open from 8 A.M. to 5 P.M. Monday through Friday, except holidays. Parking is available in the McKenzie parking lot on the west side of the building.

All shop services are available on a first-come, first-served, carry-in basis. On weekdays, bring your computer equipment to 151 McKenzie Hall and check it in with the receptionist.

Weekends. UO Bookstore customers can also drop off equipment from 10 A.M. to 6 P.M. Saturday and from noon to 6 P.M. Sunday at the Bookstore's "Digital Duck" department. The E-Shop will call you when the work has been completed, and you may pick up your machine at the reception desk in 151 McKenzie Hall.

Who to Contact. If you have any questions concerning repairs or upgrades, send an email message to *hardwarehelp@oregon.uoregon.edu*, or call **346-3548**.

Compact USB Flash Drives Offer Nifty Storage Solution

Lightweight USB Flash Drives are a handy backup-and-go solution. These colorful translucent drives are small enough to fit in your pocket and can be plugged into any USB port. No power supply or cables are needed.

Despite their toy-like appearance, the drives have a lifetime of up to one million rewrites and can retain data for up to 10 years.

The E-Shop stocks USB thumb drives in a variety of sizes: 16MB ($15), 32MB ($22), 64MB ($35), 128MB ($40), 256MB ($55), and 512 MB ($110). In addition, the shop sells 1GB *bootable* USB Flash Drives for $175 each.

Detailed product information is available on the vendor's website:
http://usbkeydrive.com/USB_Drive.htm

Build Your Tech Skills with 'Workshops-to-Go' from the Computing Center Documents Room

Vickie Nelson
Documents Room Librarian
vmn@uoregon.edu

No time to fit a workshop or class into your busy schedule? Consider taking a video workshop on VHS tape or CD-ROM.

The Documents Room Library on the ground floor of McKenzie Hall provides a restful atmosphere for browsing and study.

The Documents Room Library (175 McKenzie) has a growing collection of training materials covering such popular applications as Photoshop, Dreamweaver, Flash, InDesign, Illustrator, and the various Microsoft Office products, as well as the Mac OS and Windows operating systems. These tapes and CD-ROMs are video-based tutorials that include several hours of instruction by skilled software training experts. The CDs feature high-quality visuals, especially noticeable in the shots of computer screens.

Among our most recent acquisitions are several books from the Apple Training Series, including *Mac OS X Help Desk Essentials* and *Desktop and Portable Systems: A Guide to Supporting, Servicing, and Troubleshooting Apple Computers*; *SpamAssassin*; and *A First Look at SQL Server 2005 for Developers*.

To see a complete list of the training CD-ROMs and videos, go to **http://docsrm.uoregon.edu/** and type "training." Then hit "search."

Books and magazines. In addition to its collection of videos and CD-ROMs, the Documents Room offers books and magazines on a wide range of computing topics including computer security, Linux, Java, handheld computers, and web design and creation. You can search its catalog 24 hours a day at **http://docsrm.uoregon.edu/**

Books circulate for two weeks, videos and CD-ROMs for one week, and magazines for two days. All materials are renewable, unless another patron has requested the item.

Contact Information. The Documents Room is open 9:30 A.M. to 5 P.M. Monday through Friday. Call **346-4406** for more information or visit the Documents Room website at **http://darkwing.uoregon.edu/~docsrm/**

Updated MathType CDs Available in the Docs Room

The latest versions of MathType for Mac and PC are now available for checkout in the Documents Room.

MathType, a full-featured equation editor for Microsoft Word, is site-licensed by the UO for use by UO faculty, staff, and students. You can use it to create mathematical notation for word processing, web pages, desktop publishing, presentations, and for TeX, LaTeX, and MathML documents. The tool's web capabilities allow you to create high-resolution mathematical equations that display beautifully on web pages across browser platforms and add color to all or part of your equations—a feature that may be desirable in PowerPoint presentations.

How to obtain your copy. As long as you are a UO faculty or staff member or a currently enrolled student, you may install MathType at work and at home. Bring your UO photo ID to the Computing Center's Documents Room Library (175 McKenzie) and check out a MathType CD. You may want to call first (**346-4406**) to make sure a copy is available.

Need help? If you have questions about how to install and use this software, contact Robin High (**346-1718**, *robinh@uoregon.edu*). For more information about MathType, see **http://dessci.com/en/products/mathtype/** and **http://www.mathtype.com/en/products/mathtype/**

Large Timesharing Systems at the UO

Find out what system resources are available to you

Faculty/Staff

Faculty and staff will normally use Darkwing, a large shared Sun Enterprise 5500 Unix system targeted for email and web access.

Those needing to run compute-intensive applications may sign up for an account on the Opteron cluster, four dual processor 64-bit AMD Opteron workstations running Red Hat Linux. For more information, see **http://acad-cl0.uoregon.edu/** ("acad dash cee el zero dot uoregon.edu")

Undergraduate Students

Undergraduate student accounts are automatically created on Gladstone, a large Sun Enterprise 5500 Unix system.

Among other things, Gladstone accounts can be used for electronic mail and serving personal web pages. We also offer an expanded range of academic software on Gladstone, such as SAS and Mathematica (see software chart on page 11).

Graduate Students

Graduate students automatically have accounts created for them on Darkwing; they can also create an account on Gladstone if they wish.

Administrative Systems

Daisy. Daisy is a large Alpha administrative system running OpenVMS/AXP. The primary application running on Daisy is Banner, an administrative application environment based on Oracle, a popular large system database. Access to Daisy is restricted to staff members who are performing administrative tasks such as grade processing and payroll. For more details on administrative systems, see the Administrative Services website at **http://ccadmin.uoregon.edu/**

Off-Campus Access

Your account on Darkwing or Gladstone enables you to dial in from off campus to the university's modem pool (see "What About Off-Campus Connections?" on page 4.) The modem number for accessing UOnet, the campus network, is **225-2200.** (Note: Your modem access is for casual use—no more than a few hours a day on average. If you need dedicated or near-dedicated network access, you will want to contact a commercial Internet Service Provider. One list of ISPs is available at **http://www.thelist.com/)**

DSL and cable modem subscribers can connect via the UO's Virtual Private Network, or VPN (see **http://micro.uoregon.edu/getconnected/vpn_overview.html**). Software to access the Internet and campus facilities from home is available on the Duckware CD-ROM, which is free to all faculty, staff, and registered students (see article on page 2). You may also acquire shareware from the Computing Center's public domain libraries (**http://micro.uoregon.edu/pd/**).

Special Accounts for Classes and Departments

If you're teaching an undergraduate class and your students need to access software available only on Darkwing, temporary accounts can be created for their use. For more information, contact Connie French at **346-1738**.

Departments or university-recognized institutes, labs, or organizations can arrange for a departmental account. Such accounts are offered solely to provide an authoritative and unchanging home for departmental web pages and official departmental email, and must be officially requested by the department head or institute administrator. Contact Connie French at **346-1738** for more information.

Acceptable Use. Finally, please note that all use of university computing resources is subject to the university's Acceptable Use Policy, which is available in printed format from the Computing Center Documents Room (175 McKenzie Hall), or online at **http://cc.uoregon.edu/policy/**

Large Systems Help

If you have questions about using the UO's large timesharing computers, contact the large systems consulting group in 225-239 Computing Center (**346-1758**, *consult@darkwing* or *consult@gladstone*). They can help with questions about email, multimedia delivery, scientific and CGI programming, and web page development. To learn more, go to **http://cc.uoregon.edu/unixvmsconsulting.html**

Site-Licensed Software

The UO has site licenses for a number of software packages you can use on your campus workstation, including:

- **Norton Antivirus.** Available on the Mac Duckware 2004 CD and issued on a separate CD for PC users (see Duckware article on page 2). See also **http://www.symantec.com/avcenter/**
- **SAS.** SAS users may install SAS on their PCs both at work and at home. Go to **http://sas.uoregon.edu/**
- **Mathematica.** See **http://darkwing.uoregon.edu/~hak/mathematica/**
- **ESRI** (GIS and mapping software such as ArcInfo, ArcView). See **http://esri.uoregon.edu/**
- **MathType** (equation editing software for Mac and PC). See **http://www.dessci.com/**
- **Respondus** (a Windows application for UO-affiliated instructors who use Blackboard's exam and survey tools). See **https://blackboard.uoregon.edu/local/respondusbb/**

A full list of site-licensed software is online at **http://cc.uoregon.edu/sitelicense.html**

Statistics Consulting

If you need help with a statistical analysis project, make an appointment with Robin High, the Computing Center's resident statistical consultant. (**346-1718**, *robinh@uoregon.edu*). You may also want to visit Robin's statistical resources page at **http://darkwing.uoregon.edu/~robinh/statistics.html**

Software on Darkwing, Gladstone, Opteron Cluster

Type of Software	Darkwing	Gladstone	Opteron
Statistics Packages	sas, eqs lindo, bmdp spss, rats/estima Splus, minitab	sas, eqs spss, bmdp Splus, rats/estima minitab	R statistical system
Text Editors	pico vi emacs and xemacs eve	pico vi emacs and xemacs eve	vi jed joe emacs, xemacs
Network Software	ftp (remote file transfer) lynx (web browser) pine (email) trn, tin, nn (USENET News) ssh (secure login) pgp (encryption) spam assassin	ftp (remote file transfer) lynx (web browser) pine (email) trn, tin, nn (USENET News) ssh (secure login) pgp (encryption) spam assassin	ftp lynx links ssh
X Windows Only	netscape (web browser) xv (image manipulation) openoffice (Office Suite) acroread (Acrobat Reader) gimp	netscape (web browser) xv (image manipulation) openoffice (Office Suite) acroread (Acrobat Reader) gimp	Complete Gnome 2.6 desktop environment Complete KDE 3 desktop environment Mozilla Firefox
Programming	cc and gcc c+ and g++ f77, f90, f95 (FORTRAN) pc (Pascal) NCAR fortran graphic libs Java developer's kit tcl/tk	cc and gcc c+ and g++ f77, f90, f95 (FORTRAN) pc (Pascal) NCAR fortran graphic libs Java developer's kit tcl/tk	gcc 3.3 and 2.96 g77 J2sdk
Mathematics	mathematica,magma matlab, maple	mathematica matlab	Mathematica
Miscellaneous	TeX and LATex RealAudio server Adobe Acrobat distiller	TeX and LATex RealAudio server Adobe Acrobat distiller	

On the Road? Access Your UO Email via Secure UO Web Email at http://email.uoregon.edu/

Your UO computing account gives you access to secure, SSL-encrypted webmail at **http://email.uoregon.edu/**

UO web email is a good choice for new students and others who access their email from multiple locations. To use it, just open your web browser to **http://email.uoregon.edu/** and choose Gladstone or Darkwing as your email server. Enter your UO computing account username and password in the dialog box that opens, and you're on your way!

You can use UO webmail in addition to your other favorite email clients like Eudora or Mac OS X Mail without worrying about messages being moved around as they're read. For example, if you read and save Monday's mail with UO webmail, you'll be able to find all the messages you saved if you decide to open your mail with Eudora on Tuesday.

For step-by-step instructions on using UO web email, as well as links to frequently asked questions about using email at the UO, see **http://cc.uoregon.edu/email.html**

Cyberwars: Where Do We Go From Here?

The role of Microsoft's XP Service Pack 2 in the ongoing fight to virus-proof Windows

Dan Albrich
Manager, Microcomputer Services
dalbrich@uoregon.edu

Last fall the campus was hit hard with the likes of Blaster, Welchia, and Sasser, just to name a few. We all knew that anyone could get a virus by downloading a suspicious file or opening an email attachment, but few realized that our Windows computers could be infected simply by connecting to the Internet.

During the height of the campus contagion, we saw cases of people becoming infected while booting their PCs—even with firewalls enabled—because there was a 10-second lag between the time the PC connected and the firewall became effective. Worse still, new computers with integrated wireless cards could be infected simply by being turned on within range of a wireless access point.

Each of the viruses that wreaked such havoc last fall specifically targeted Windows vulnerabilities and left other platforms unaffected. In addition, Microsoft Outlook has been found to be an integral component in the propagation of the more common type of email-based viruses called "worms." All of this is bad news for Microsoft, and has users and computer support staff worldwide scrambling to come up with answers.

Microsoft responds: Windows XP Service Pack 2 (SP2)

After spending approximately one billion dollars on development, Microsoft recently released the largest update to Microsoft Windows ever. Much of this update, called "Windows XP Service Pack 2," is designed to patch holes or vulnerabilities in Microsoft Windows in hope of reducing the current onslaught of worms, viruses, and spyware affecting Windows users.

Should I install it?

There's no magic bullet that can guarantee computer security once and for all. However, SP2 does address the specific vulnerabilities that enabled Blaster, Welchia, and Sasser to take hold. For those of you who haven't installed this critical set of updates, we strongly encourage you to do so. History has taught us that the time lag is shortening between the release of a patch for a particular vulnerability and the creation of a worm or virus that exploits it. In other words, choosing not to apply new patches as soon as they are released seems to directly result in your PC becoming virally infected.

What's new in SP2?

- **Network Protection:** The main change here is an integrated firewall that works. Microsoft eliminated the 10-second lag between the time a network connection became active and the time the integrated firewall became effective. Firewalls keep your computer safe from random unsolicited network connections from arbitrary Internet hosts. The firewall does not stop you from running network applications such as browsing the web, or getting your email. It simply stops any unsolicited inbound network connections.
- **Memory Protection:** This feature blocks attacks that try to copy too much data into areas of your computer's memory. This form of attack, called a buffer overrun, is a common means of gaining unauthorized access to computing systems or denying access to legitimate users. SP2 supports a hardware feature called DEP (data execution prevention) that is supported on some microprocessors. This feature marks certain memory locations as data only, and subsequently blocks exploits that utilize execution of data as executable code.
- **Other protections designed to limit the spread of email viruses, and those contracted through browsing the web:** SP2 also includes updates for tablet and multimedia versions of Windows. Microcomputer Services staff recommend that you use an alternate browser (*not* Internet Explorer) for your general purpose browsing needs. For this reason, Duckware 2004 automatically offers to install Firefox, a good alternative browser, if you do not appear to have something other than IE installed.

How do I get SP2?

You can download SP2 via Windows Update if you have a high-speed Internet connection (for example, if you're on campus or have a DSL or cable modem).

References

"Securing Windows":
http://micro.uoregon.edu/security/windows/index.html

"Features and Functionality in Windows XP Service Pack 2":
http://www.microsoft.com/technet/prodtechnol/winxppro/plan/xpsp2ff.mspx

PC Magazine article "Windows XP Service Pack 2":
http://www.pcmag.com/article2/0,1759,1631045,00.asp

'I Think I Have a Virus…What Do I Do?'

Learn the basics for cleaning up your system and making sure it stays secure

If your PC begins crashing frequently, restarting spontaneously, or otherwise acting strangely, it's likely that your machine is either afflicted with spyware or infected with a virus. If the Computing Center detects a virus on your computer, you'll be notified via email and your network connection may be disabled until the virus is eradicated.

If you suspect you have a virus, or if you've been notified that you have one, what can you do? Below are some basic steps you can take to find and eradicate a virus.

How to detect a virus

- Install Norton AntiVirus (NAV) if it's not already installed.
- If you're using a Windows PC, insert the Windows Security CD. When the program starts, read the information displayed in each window. If you're unsure which option to select, press the ENTER key to choose the default option.

  (The Windows Security CD will enable a firewall if available, enable automatic Windows Updates, install specific critical patches, update virus definitions, and start a NAV scan. The Security CD can also help clean up spyware problems, should you have them.)
- Scan with NAV (if you're a Windows user, the Windows Security CD will do this for you, as described in the preceding paragraph). NAV should find the virus(es) and remove them. There is no need to watch the scan, but pay careful attention to the scan results.
- Scan again until the report comes up clean. If NAV gets "stuck" and keeps finding the same virus, see "What if NAV finds one or more viruses…?" below.

What if NAV finds nothing?

If your network connection has been disabled because we detected a virus on your computer, then NAV should find something. An antivirus scan that finds nothing usually means that your virus definitions file is not up-to-date (see "Live Update Expired?" at the bottom of this page).

What if NAV finds one or more viruses but doesn't fix the problem?

If your antivirus program identifies an infected file but does *not* quarantine, delete, or fix it, reboot your system in Safe Mode and do a full system scan for viruses. To enter Safe Mode in Windows, restart your computer while holding the F8 key. If necessary, contact Microcomputer Services for advice.

What if I can't get the virus definitions date to change?

This is a common problem. The usual cause is that your LiveUpdate subscription has expired. We can give you a renewal subscription code free of charge (see "LiveUpdate Expired?" at the bottom of this page).

What if I can't get the NAV window to appear at all?

This is also a common problem. Some viruses block NAV from installing or running. Contact Microcomputer Services for advice.

Note: If you feel you are incapable of removing the virus yourself, please turn your computer off until technical support can assist you. ***We strongly recommend not using a machine that is virally infected.*** The longer a virus is on the system, the more damage it can do to your files. Extremely malicious viruses that delete or modify files on compromised systems not only cause problems for you, but due to their potential access to network shares they can also modify, delete, and infect files belonging to others.

Contact information:

Microcomputer Services is located on the ground floor of McKenzie Hall in Room 151 and is open weekdays from 9 A.M. to 5 P.M. You can reach their office by phone (**541-346-4412**) or email (*microhelp@uoregon.edu*). For general microcomputing advice as well as valuable troubleshooting and security tips, visit their website at **http://micro.uoregon.edu/**

Has Your Norton AntiVirus LiveUpdate Subscription Expired?

If you're getting messages that your UO Norton AntiVirus subscription has expired, don't worry. You can renew your subscription easily. Here's how:

Connect to UOnet (the campus network) and go to **http://micro.uoregon.edu/av/** Click on the link "Virus Definition subscription codes for Live Update." This link takes you to a page where you can find the appropriate code for your system. (Note that this link can be accessed *only* from a UO connection.) Instructions for entering the code are available under "Norton Antivirus" on our antivirus information page at **http://micro.uoregon.edu/av/**

Try These Alternative Web Browsers For More Pleasant Websurfing

Spencer Smith
Microcomputer Support Specialist
spencera@uoregon.edu

If you're plagued by popups and your computer is slowed by adware and spyware, try Firefox, Mozilla, or Opera for a more trouble-free browsing experience

Over the past few years, advertising firms and other companies have made browsing the Internet increasingly annoying. The popup advertising, spyware, and malware that some web pages push onto your computer compromise your privacy, security, and your computer's stability. There are some recovery tools available, like SpyBot and AdAware, but it would be better to keep these intrusive programs off your computer entirely.

Because of the way Microsoft Windows is designed, Microsoft Internet Explorer is deeply embedded into Windows. This allows spyware and adware deep access to the Windows operating system. In addition, Internet Explorer has "features" that are exploited by the spyware authors, such as ActiveX and other integrated scripting operations. Since IE comes with every copy of Windows, it's easy for the spyware authors to assume those features are present and active.

There are several alternative web browsers that have fewer vulnerabilities. Firefox, Mozilla, and Opera are excellent choices to replace IE. Not only do they lack the deeply embedded hooks that are built into IE, they have several other features that make them advantageous.

Firefox, Mozilla, and Opera all have built-in popup blocking. With this feature turned on, most of the more common popup windows simply fail to pop up, totally eliminating the pesky in-your-face advertisements. Since those popup ads often carry their own spyware and adware, an intrusive popup window can lead to a cascade of unwanted windows, all installing and running their own spyware and increasing the load on your computer. *(Note: While it is true that IE now also blocks popups under XP S2, it continues to be plagued with other serious issues. See "Security Alerts" on page 18.)*

Mozilla comes with an email program, news reader, and other enhancements that make it a good choice for those needing a full-featured web browser. When Netscape was bought by AOL, the coding team branched out and created Mozilla. Based on the same code base, it incorporates most of the features of Netscape without being a corporate-owned product.

Firefox is a light, small, fast browser that has all the standard features. Made by the same people who created Mozilla (and Netscape as well), it's a great browser for those who don't need all the clutter, features, and add-ons that IE and Mozilla provide.

Opera advertises itself as the "fastest browser on Earth." It's snappy and feature-rich. The free version does integrate ads into the menu bar, however. To get rid of the ads, you need to pay for the product. Still, as a light, fast browser, Opera has many advantages.

If you're plagued by popups and your computer is slowing down from its load of adware and spyware, you may want to consider one of these alternate browsers.

References

For more information on Mozilla, Firefox, and Opera, see the following websites:

- Mozilla: **http://www.mozilla.org/**
- Firefox: **http://www.mozilla.org/products/firefox/**
- Opera: **http://www.opera.com/**

Who is Ernestine—and How Can 'She' Help You?

Dial **6-0000** from any campus phone and the voice recognition directory known as 'Ernestine' will route your call to a UO staff member or department after you speak the name. If you dial **6-0003**, Ernestine will also provide their email addresses.

Ernestine service is available 24 hours a day. If you're calling from off-campus, you can access the phonetic directory by dialing **541-346-6000**.

For more information, visit the Telecommunications Services' page at **http://telecom.uoregon.edu/ernestine.htm**

Looking Forward:

New Services at the UO Libraries this Fall

Ron Renchler
Director, Library Communications
UO Libraries
ronr@darkwing.uoregon.edu

Several new and expanded technology-related services will be available at the UO Libraries this fall. Updates on new library services are posted frequently in the *News* section of the library's website at **http://libweb.uoregon.edu/news/whatsnew/** Here's a short list of what's on tap for fall:

Instructional Technology Directory

The UO Libraries Interactive Media Group recently launched a new web resource (**http://itdirectory.uoregon.edu/**) that matches educational technology users with relevant services. Targeted primarily at instructors, the Instructional Technology (IT) Directory project is a direct response to faculty requests for a comprehensive, user-friendly guide to the many educational technology service providers scattered across the UO campus. The design emphasizes nontechnical terms and carefully developed category searching, so users can find the help they need even if they aren't familiar with the latest ed tech jargon and organizational labels. If you'd like to have your technology service included in the directory, contact project manager Kirstin Hierholzer (**346-1995**, *kirstinh@uoregon.edu*).

Scholars' Bank

UO faculty members are encouraged to use the newly developed *Scholars' Bank* at **http://scholarsbank.uoregon.edu/** *Scholar's Bank* is an institutional archive for UO research in digital form, including preprints, technical reports, working papers, student terminal projects, datasets, and more. It's a tool for collecting, disseminating, and preserving the intellectual output of the UO community. Built around the concept of research communities, *Scholars' Bank* gives users easy remote access and the ability to read and search items generated at the UO from one location: the World Wide Web. The service offers standardized digital preservation presentation, and distribution of many forms of data, including text, audio, video, images, datasets, and more. Interested faculty should contact the coordinator of the project, Carol Hixson (*chixson@uoregon.edu*, **346-3064**), for information on how to establish a community for their research.

New Digital Collections

The Metadata and Digital Library Services department in the UO Libraries has been hard at work during the past year expanding the library's ever-growing digital collections. Several new collections have recently been made publicly available, including *Picturing the Cayuse*, *Historical Photographs*, *Western Waters*, and the aforementioned *Scholars' Bank*. Several others will be coming online soon. All public digital collections can be accessed at **http://libweb.uoregon.edu/catdept/digcol/index.html**

New Databases and Electronic Resources

The library continues to add powerful new databases and other electronic research aids to its collections. Many new databases are being acquired through the library's collaborative efforts with other Oregon libraries to license databases for statewide use through a single vendor, EBSCO Publishing. The new program, administered by the State Library in Salem, saves the state nearly $10 million annually in database licensing fees.

In the past year, the following databases were added to the library's collections as a result of its participation in the program: *Alt HealthWatch*, *Computer Source*, *Legal Collection*, *Military and Government Collection*, *Professional Development Collection*, *Psychology and Behavioral Science Collection*, *Religion and Philosophy Collection*, and *Vocational and Career Collection*. These databases typically provide full-text content for several hundred journals in each discipline.

Other databases or upgrades acquired individually by the UO Libraries in the past year include *All Academic*, *Chicano Database*, *FIAF—International Film Archive*, *SourceOECD*, and *Web of Science*. More information on the library's databases is available at **http://libweb.uoregon.edu/dbs/indexes.php**

Access to Articles in Psychology

If you're looking for full-text articles in psychology and related fields, you'll be happy to know that the library has added full-text online access to the contents of 53 journals (**http://www.apa.org/psycarticles/covlist.html**) published by the American Psychological Association and its affiliates. To access the full text of an article of interest from these journals, click the *FindText* button on the library's home page at **http://libweb.uoregon.edu/** and conduct a FindText search for the article. The results will provide links to full-text versions.

Labor History Site Launched

Researching labor history using materials in the UO Special Collections and University Archives became much easier with the launch of *The Labor Project*, a new web resource that includes a searchable online catalog of major holdings in the labor history collection. To use the new resource, visit **http://libweb.uoregon.edu/speccoll/exhibits/labor/index.html**

UO's New Online Travel Reimbursement Form Streamlines Payment Process

The form's success sparks keen interest in the Banner world

Joyce Winslow
jwins@uoregon.edu

Campus Business Services Associate Director Nancy Cameron, Assistant Director Krista Borg, and systems programmer Joey Mitchell, three of the principal collaborators in the creation of the UO's new online travel reimbursement form, share a light moment. Borg and Mitchell will demonstrate the form's virtues at the Banner users' SETA West Conference in Seattle this fall.

Ask campus staff what they think of the new UO online travel reimbursement form, and they're likely to sum it up in one word: "Quicker!"

The new web-based form, which may be accessed from DuckWeb by any authorized department staff member, enables employee travel reimbursements to be processed largely in-house, eliminating the need for data entry and a lengthy review and approval process by the UO Business Office. The result: travel reimbursements are processed in a matter of *days* instead of weeks. And after they're approved, reimbursements can be directly deposited into an employee's bank account, eliminating the time and cost involved in issuing checks.

Another time-saver is the built-in *per diem* calculator, which instantly computes lodging and food expenses for any locale in the world. In addition, official regulations governing travel expenses are automatically updated and applied, eliminating the need to spend time researching and interpreting the rules, and expediting the final approval process.

The new module is the product of close collaboration between Business Office administrators Nancy Cameron and Krista Borg, and a Computing Center programming team led by Joey Mitchell—as well as many other Business Office and department personnel on campus who gave important feedback on its design.

The design team's goal was to create a product that conformed to regulations, contained all the necessary information, and yet was simple enough that anyone could easily learn to use it. During the twelve months it took to create and test the form, programmer Joey Mitchell says he kept two thoughts uppermost in his mind: "Think of everything!" and "Keep it simple!"

Business Office staffers Nancy Cameron, Krista Borg, and Carolyn Wooley continue to devote a large percentage of their time to training department personnel to use the travel form. Since its debut in September 2002, more than 200 UO staff in 120 campus departments have been trained to use it, and approximately 15,000 forms have been processed online.

Cameron and Mitchell first presented the travel form to some 350 colleagues at the March 2004 SCT Summit Conference in Philadelphia. It was so well received that Banner developer SunGard SCT has expressed an interest in incorporating the module into its product line. This fall, Mitchell will again demonstrate the form, this time in tandem with Krista Borg, at the regional Banner users' group (SETA West) in Seattle.

Department personnel interesting in signing up for training in the use of the new web-based travel form should contact Judy Fossum (*baojudy@uoregon.edu*, **346-2387**). Trainings are currently being scheduled every other month; the two half-day sessions include testing, and those who wish may extend their training to include the full certification necessary for creating invoices online.

« cybercrime in the news »

"Phishing" Continues to Net Unwary Consumers

Fraudulent emails designed to glean sensitive personal information that could be used in identity theft are still fooling one out of three Internet users. For details, see
http://www.msnbc.msn.com/id/5519990/

Telecom Fraud Leaves No Sector Unscathed

Using schemes ranging from low-level subscription fraud to sophisticated database break-ins, thieves are using fraudulent access to networks to steal services, and no sector of the telecom industry remains untouched. For details, see
http://www.billingworld.com/archive-detail.cfm?archiveid=7575

Florida ID Theft Case Levies Record 144-Count Indictment

A Boca Raton man is accused of stealing vast amounts of personal information from Acxiom Corporation, resulting in losses of more than $7 million. For details, see
http://www.cnn.com/2004/LAW/07/21/cyber.theft/index.html

DDoS Attacks Become Extortionists' Tool

Organized, crippling denial of service (DDos) attacks are the latest weapon in cybercrime. In what is being called the first criminal case arising from a DDoS-for-hire scheme, a Massachusetts businessman has been charged with paying members of the computer underground to launch DDoS attacks against his competitors. For details, see
http://www.securityfocus.com/news/9411

SEC Warns of "Wrong Numbers" Fraud

If you find a "hot" stock tip on your answering machine from someone you don't know, notify the SEC. This new scam is a deliberate attempt to deceive people into thinking that the caller misdialed and that their "tip" was intended for someone else, inspiring the unwary to invest in a particular stock. For details, see the government report at
http://www.sec.gov/investor/pubs/wrongnumberscam.htm

Lone 419 Spammer Convicted in Dutch Case

Of the 50 suspects arrested earlier this year in an extensive anti-spam raid in Amsterdam, only one was successfully prosecuted and sentenced to 12 months in prison. For the full story, see
http://www.theregister.co.uk/2004/08/17/one_419er_jailed

New FTC Email Address for Reporting Spam: *spam@uce.gov*

To lodge a complaint against spammers, consumers should now contact *spam@uce.gov* Remember to include the full email header in your complaint. To learn more about how to avoid spam scams, go to
http://www.ftc.gov/spam/

South Korea Now Leads as Spam Capital

In August, average spam outbreaks surpassed 600,000 per day. Nearly half (47%) of these originated in South Korea, making that country the new world leader in spam hosting and a close second in spam distribution. For details, see
http://www.tmcnet.com/usubmit/2004/sep/1069591.htm

Illegal File Sharing Under Fire

On July 27, a federal judge affirmed that copyright holders had the right to unmask anonymous file swappers accused of copyright violations. This ruling gave the Recording Industry Association of America (RIAA) an important tool for prosecuting music pirates. For the full story, see
http://zdnet.com.com/2100-1104-5285605.html

In another action, a group of 46 state attorneys general asked file-sharing companies to take stronger action on privacy and intellectual-property violations. For details, see **http://zdnet.com.com/2100-1104_2-5298413.html**

Internet Prescription Scammers Plead Guilty

Two Florida siblings accused of illegally distributing drugs over the Internet plead guilty recently to the charges brought against them by the FDA. The pair, a brother and sister, had operated websites and toll-free numbers through which they unlawfully distributed and dispensed controlled substances without a prescription. Vincent Chhabra faces the possibility of 33 months of jail time, while his sister was sentenced to 12 months probation. For details, see
http://www.fda.gov/bbs/topics/news/2004/NEW01112.html
http://www.boston.com/news/nation/articles/2004/09/02/fla_duo_plead_guilty_to_fraud_drug_sales/

'Zombie' PCs Spew Spam

The latest trend in cybercrime is to write malicious programs designed to hijack PCs and create a network of 'zombies' —computers that can be used without their owners' knowledge to run programs of the hackers' choosing—and then sell these zombie networks to spammers and identity thieves. In recent months, this practice has contributed to record increases in web contagions and spam-related crimes. See
http://www.usatoday.com/tech/news/computersecurity/2004-09-08-zombieuser_x.htm

China Authorizes Life Sentences for Some Porn Peddlers

The Chinese government recently authorized harsh measures against those who peddle pornographic material over the public networks. Depending upon the severity of the case, perpetrators can expect sentences ranging from detainment to life in prison. See
http://www.chinatechnews.com/index.php?action=show&type=news&id=1733

Security Alerts…

— Microsoft Windows—

Be Sure to Apply XP S2 via Windows Update!

Dialup Users: Use This Link to Order Windows XP Service Pack 2 on CD

Microsoft has provided a link specifically for dialup users who wish to order the new Service Pack 2 on CD. Microsoft will ship the CD, which contains the same Service Pack 2 software that is available for download from its Windows Update site, free of charge:

http://www.microsoft.com/windowsxp/downloads/updates/sp2/cdorder/en_us/default.mspx

Important Cumulative Update for Internet Explorer

Internet Explorer users are urged to immediately apply Microsoft's latest cumulative critical security update (**MS04-025**). This update, which includes corrections for Windows XP users who are running Windows Update Version 5, addresses three serious vulnerabilities in Internet Explorer. 5.*x* and 6 that may allow attackers to execute malicious code on a victim's computer.

References:

http://www.microsoft.com/technet/security/bulletin/ms04-025.mspx

http://www.us-cert.gov/cas/techalerts/TA04-212A.html

http://www.internetnews.com/security/article.php/3388561/

Serious Winamp Vulnerability

In late August, Secunia's security team reported an "extremely critical" flaw affecting Winamp that can be exploited to compromise users' systems without their knowledge. *Internet Explorer users are particularly vulnerable.* For details, see
http://secunia.com/advisories/12381/

Finding Microsoft Security Downloads

To search for patches for Microsoft products, go to the Microsoft Download page at

http://www.microsoft.com/downloads/search.aspx?opsysid=1&search=Keyword&value='security_patch'&displaylang=en

MyDoom Mass Mailing Plague Continues

Windows users are urged to update their virus definitions

In late July, MyDoom-O made headlines when it caused big headaches for Google, Yahoo, and Lycos. This particular worm, which scanned domains of the major search engines for email addresses, had the effect of a DDoS attack, disrupting Google service worldwide and infecting vulnerable PCs with its malicious executable files.

Since then, there have been more than a half dozen new variants of the worm, all of which affect only Windows PCs (95/98/Me/NT/XP). One of the variants (MyDoom-Q) runs a backdoor trojan called Backdoor.Nemog, which allows an infected computer to be used as an email relay and HTTP proxy.

Users should be aware that these worms may also be distributed via P2P (peer-to-peer networks), IM (Instant Messenger) channels, and the like.

Current information on MyDoom and other viruses is available at Symantec's Security Response site:
http://securityresponse.symantec.com/avcenter/vinfodb.html

Beagle/Bagle Variants Spreading Through Spam

Hundreds of thousands of emails containing the word "price" flooded inboxes with record speed as the latest variant of the Beagle (aka Bagle) virus hit the networks in August.

Like the MyDoom worms, Beagle may also be distributed via P2P and IM resources. Also like MyDoom, Beagle attacks only Windows machines, underscoring the need for Windows users to be scrupulous in keeping their virus definitions up-to-date.

Removal tools for W32.Beagle variants are on Symantec's Security Response site at
http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle@mm.removal.tool.html

'Highly Critical' AOL Instant Messenger Flaw

A serious flaw in AOL Instant Messenger's "Away" message handling system leaves users open to attack, allowing intruders to hijack a user's system and run malicious code. For details, see Secunia Advisory SA12198 at **http://secunia.com/advisories/12198/**

Yahoo Issues Instant Messenger Patch

In mid-August, Yahoo issued a security patch to fix a vulnerability in its latest version of Instant Messenger (IM). At issue is the way its Instant Messenger software handles PNG graphics, potentially allowing malicious programs to be executed when a vulnerable application loads an image. Information about the patch is available from the Yahoo Messenger site at
http://messenger.yahoo.com/security/update5.html

For more details, see
http://zdnet.com.com/2100-1105-5309129.html

ActiveX Control Buffer Overflow Vulnerability in Adobe Acrobat 5.*x*, 6.*x*

This vulnerability in Adobe Acrobat/Acrobat Reader can allow attackers to execute arbitrary code and take control of the affected system. To learn more, see the iDEFENSE Security Advisory at

http://www.uniras.gov.uk/l1/l2/l3/brief2004/brief-43804.txt

— Other Alerts —

MIT Kerberos 5 Vulnerabilities

Systems running versions of Kerberos 5 libraries prior to krb5-1.3.5 are vulnerable to several kinds of attack, the worst of which could allow arbitrary code execution by an intruder, compromising an entire Kerberos realm. For details, see US-CERT Alert TA04-247A at

http://www.us-cert.gov/cas/techalerts/TA04-247A.html

Bluetooth Flaws Expose Mobile Phone Users to Attack

Victims of exploits of Bluetooth technology in mobile phones could have their privacy seriously violated: address books, calendars, text messages, and even private phone conversations could all be exposed to the prying eyes and ears of attackers. The Nokia 6310 and 8910 series and the Sony Ericsson T610 are particularly vulnerable to attack because of their popularity. Manufacturers are aware of the problem and are taking steps to improve the security of their products.

For details, see *Wired's* August 6 article, "Security Cavities Ail Bluetooth," at

http://www.wired.com/news/privacy/0,1848,64463,00.html

PNG Security Issues Affect Mac OS X Mail, Mozilla, Linux, Windows

In August, six vulnerabilities were reported in common code supporting the portable network graphics (PNG) format. If left unpatched, the most critical of these could trick victims into visiting a malicious website and trigger a buffer overflow. For more information about the problem and its fixes, see

- **http://www.libpng.org/pub/png/libpng.html**
- **http://www.us-cert.gov/cas/techalerts/TA04-217A.html**
- "Image Flaw Pierces PC Security" : **http://news.com.com/Image+flaw+pierces+Linux+security/2100-1002_3-5298999.html**

PuTTY 0.55 Fixes Serious Security Hole

PuTTY, a free Telnet and SSH client for Win32 and Unix platforms, has a serious security hole that may allow attackers to spoof server identities to run malicious code. Users are urged to update to PuTTY 0.55 to correct the problem. The update was released August 3. UO users may download it from Public, the public software server maintained by Microcomputer Services at

http://public.uoregon.edu/software/Network Software/SSH/

Look for the file **putty.zip**

Netscape/Mozilla Vulnerabilities

Multiple vulnerabilities have been found in Mozilla packages for Red Hat Linux 1.4.3 and, most recently, in Netscape 7.2 for Windows and Netscape 7.*x* Most of the attacks are perpetrated by tricking users into visiting malicious web pages.

In August, Red Hat issued fixes for nearly a dozen of these flaws (see **http://www.linuxsecurity.com/advisories/redhat_advisory-4640.html**). The Netscape 7.*x* vulnerabilities are related to flaws affecting Mozilla software. For details, see **http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1006326,00.html**

Windows users: Instructions for updating Mozilla, Firefox, and Thunderbird are available at **http://mozilla.org/security/shell.html**

High-Risk Bug in Mplayer GUI

Mplayer, which comes with many Linux distributions, contains a serious vulnerability in its graphical user interface (GUI) that could allow attackers to execute malicious code on a Linux or Unix system.

Users are advised to upgrade to the latest version of Mplayer, while system administrators are being urged to switch off Mplayer's GUI altogether. For details, see **http://open.itworld.com/4909/040803linuxbug/page_1.html**

Researchers Find Fault with MD5 Algorithm

Preliminary research suggests that MD5, an algorithm embedded in common security applications, may be too flawed to remain the "gold standard" in encryption programming.

Some experts are recommending that programmers discontinue the use of MD5 now, before successful attacks are devised. For details, see **http://zdnet.com.com/2100-1105-5313655.html**

Microsoft Windows XP Service Pack 2 and

How the trend in new security measures may affect the way you approach web design

Joe St Sauver, Ph.D.
Director, User Services and Network Applications
joe@uoregon.edu

By now, most users of Windows XP know that Microsoft has released a large update for its operating system called Service Pack 2 (XP SP2).

This article is not meant to focus on XP SP2 itself, but rather to alert you to potential interactions between XP SP2's new features and World Wide Web pages. You may run into these issues whether you're a web designer or simply an XP SP2 user.

The Most Noticeable Issue: Popup Windows

Perhaps the biggest issue you potentially face is associated with popup windows in Internet Explorer post-XP SP2.

Most users have become accustomed to seeing multiple windows pop up automatically when they visit a website. Sometimes the popup window may contain an advertisement you'd rather ignore, but in other cases it may contain crucial information pertaining to that website.

If you are running XP SP2 and are browsing a website that attempts to open a new popup window, you'll see an alert appear at the top of the main browser window. When you see that alert you can choose to allow the popup window to be displayed if you wish, either one-time only or on an ongoing basis.

If you are designing websites to be functional in a post-XP SP2 environment, you should assume that users will *not* allow pop up windows to be displayed, and you should design your website so that the website "fails gracefully" if and when that occurs.

While some website designers may rail against XP SP2 for "breaking popup windows," the reality is that many users may already have been running anti-popup software for some time, and XP SP2 simply makes the issue crystal clear: a popup-dependent website needs to be redesigned to *not* rely on popup windows.

I should also mention that because the top-of-the-page popup alert area is a new "priority attention" area for users, website designers—and advertisers—have already begun emphasizing the content that's delivered to that part of the web page. In addition, you can expect many sites to urge you to once again allow their own popup windows to be routinely displayed.

Active Content

The other major change that you may run into post-XP SP2 relates to active content, programs that are downloaded as part of a web page and run on the local system.

As part of its security improvements, Windows XP SP2 has dramatically reduced the types of active content that can be delivered to, and run on, end user systems. If you attempt to download and run content that doesn't meet the new guidelines, by default Internet Explorer will display a boxed red "X" instead of the potentially problematic content.

If you have a website that relies on active content, you will want to verify that your programs and scripts continue to work as expected on post-XP SP2 systems. You may also want to plan for the time when essentially no scripting or other active content works whatsoever as users continue to harden their systems against online browser-delivered security exploits.

The XP SP2 Firewall and Local Web Servers

Another security-related change associated with XP SP2 is the introduction of a default software firewall.

While the firewall will generally be transparent and non-intrusive for user-requested content "pulled" from the web, the XP SP2 firewall will normally make an XP system running SP2 unsuitable for use as a web server (or any other sort of server delivering content outbound in response to a third party's request).

Most people do *not* routinely view desktop systems running Windows XP as an appropriate operating system for server-type tasks, nor should they, but we know that some people do wild things that go far beyond what Microsoft generally anticipates or supports.

While you can disable the default firewall filtering (in general or just for specific ports) to try to make XP SP2 usable for server-type tasks, you should ***not*** do that. If you need a server, run a server-class operating system on a dedicated system, do *not* try to "make do" with Windows XP on a user desktop (and don't forget that in most cases Darkwing or Gladstone will work fine for serving routine user web page).

Browsers Other Than Internet Explorer

The other impact of XP SP2 is an indirect one: as users improve their system security, a growing number of users may elect to install and use a browser other than Internet Explorer (IE). Because IE has traditionally had a huge market share (up to 95% of the market by some estimates), many web developers have "gotten sloppy" and have designed their websites to work only with IE. For good or ill, those days of browser monoculture may be drawing to a close. For example, here at UO this fall, we are distributing Mozilla as an alternative to IE on the Duckware CD-ROM.

Again, the key message we'd like to impart is the importance of designing conservative web pages that use fundamental HTML constructs rather than exotic features which may work only on specific browsers. You should also be sure to test your website against a wide variety of different web browsers.

Conclusion

You should not allow the comparatively minor issues discussed in this article to discourage you from installing XP SP2 on your system. It is important that all users of Windows XP install (or allow Windows Update to automatically install) Service Pack 2. Regardless of whether you yourself run Windows XP, if you have web pages, you do need to take a moment to review your web pages for compatibility with Windows XP SP2, repairing any that have issues.

If you're a UO faculty member, UO student, or UO staff person and have any questions or concerns relating to Windows XP SP2 and its interaction with web pages, feel free to contact me at *joe@uoregon.edu* or **346-1720** to talk about those issues.

« sites worth seeing »

1. **"Cybersecurity research gets $7 million"…**In August, the National Center for Advanced Secure Systems Research (NCASSR) was granted $7 million for cybersecurity research. See **http://zdnet.com.com/Cybersecurity+research+gets+247+million/2110-7347_3-5302924.html**
2. **"Tech industry presents less-than-unified defense"…** If hardware and software companies joined forces to shore up cybersecurity, cleaning up the World Wide Web would not be such a daunting task.
   http://www.usatoday.com/tech/news/computersecurity/2004-09-09-zombie-response_x.htm
3. **"BBC to Open Content Floodgates"…** This fall, the BBC plans to share its professionally produced audio and video clips over the Internet, making them freely available for noncommercial viewing, sharing, and editing. Clips from the its natural history archives will be the first to be released.
   http://www.wired.com/news/culture/0,1284,63857,00.html
4. **"Windows Update"…** *PC Magazine*'s in-depth review of Windows XP SP2. Sebastian Rupley's article gives you an under-the-hood glimpse of some of the new security improvements.
   http://www.pcmag.com/article2/0,1759,1635634,00.asp
5. **US-CERT Cyber Security Bulletins…** This bi-weekly report provides a nice technical summary of current security issues. (If you're interested, you may sign up to receive these reports via email at **https://www.us-cert.gov/cas/signup.html**)
   https://www.us-cert.gov/cas/bulletins/
6. **Reiser4 Filesystem…**Learn more about this fast, atomic filesystem with military-grade security.
   http://www.namesys.com/
7. **INFOSYSSEC: "The Security Portal for Information System Security Professionals"…** A website designed to help students and security professionals locate and consolidate Internet resources pertaining to information system security.
   http://www.infosyssec.com/
8. **"Q&A: Tom Leighton, chief scientist at Akamai"…** A *Computerworld* interview concerning the DDoS attack on Akamai Technologies last spring.
   http://www.computerworld.com/securitytopics/security/story/0,10801,93875,00.html
9. **"Judges rule file-sharing software legal"…** This August 19 decision by a federal appeals court ruled that distributors of software using the Gnutella and FastTrack P2P technologies are not liable for copyright infringement committed by users of their software. The controversial ruling upheld the legality of such filesharing programs as Grokster and Morpheus.
   http://news.com.com/Judges+rule+file-sharing+software+legal/2100-1032_3-5316570.html
10. **"SpaceMonger"…** If you're a Windows user, you may want to check out this tool, which keeps track of the free space on your computer.
    http://www.werkema.com/software/spacemonger.html

An Update on Statistical Resources at the UO

Robin High
Statistical Programmer and Consultant
robinh@uoregon.edu

This article introduces you to statistical software available on Darkwing and Gladstone and statistical programs that can be loaded onto your personal computers.

In recent years the primary resources for statistical computing at the University of Oregon have shifted from the large-scale timesharing systems, such as Darkwing, to the personal computer (PC). In fact, statistical programs available for desktop and laptop computers have the computing edge for many applications.

What Statistical Programs Are Available?

The primary statistical program that's available on both Darkwing and Gladstone is SAS Version 8.2. Other programs with statistical applications that are available on both systems include Splus 6.1.2, bmdp 7.1, eqs, minitab Release 9.1, and rats 5.01. SPSS Release 6.14 is available only on Darkwing.

SAS 9.1.3 for Solaris and the PC, the most recent version of this software, has recently been delivered and will soon be installed on Darkwing and Gladstone. Version 8.2 will remain the default for several months. For details on how to install either version 8.2 or 9.1.3 of SAS on your PC, including operating system requirements, see **http://darkwing.uoregon.edu/~robinh/012load.txt**

SAS 8.2 license renewal. In the coming year you will still be able to run version 8.2 of SAS on your PC. If you would rather not install version 9.1, and if you have not already updated your license for 2005, you need to request a new **setinit.sss** file from **http://ssil.uoregon.edu/sas/** Copy this file into the program editor and run it as you would a SAS program to update the settings. *Without this license update, SAS version 8.2 won't run on your PC after October 15th.*

Important note: It is important that each year every user register his or her copy of SAS individually so that we remain in compliance with our licensing agreement with the SAS Institute, which requires us to keep an accurate count of the number of SAS users on campus. This requirement applies to individual computers, whether you are a UO student or a member of the UO faculty or staff.

SAS Documentation

The most recent documentation for SAS will continue to be available online at
http://sas.uoregon.edu/sashtml/main.htm

The master index is a quick way to look up details concerning almost any procedure, option, or keyword that is part of the SAS system. To access this web page you need to connect to the network from a campus computer or from a secure VPN connection off-campus. VPN (virtual private network) software is available from Microcomputer Services (151 McKenzie Hall, **346-4412**).

For a longer and more detailed review of statistical computing resources at the University of Oregon, please see **http://darkwing.uoregon.edu/~robinh/stat_comput.txt**

late-breaking security news

More Mozilla Vulnerabilities

On September 17, US-CERT reported a series of vulnerabilities affecting the following Mozilla products, the most serious of which could allow attackers to execute malicious code:

- Mozilla web browser and email, newsgroup clients
- Firefox web browser
- Thunderbird email client

See **http://www.us-cert.gov/cas/techalerts/TA04-261A.html**

Windows Flaw Afflicts Office XP 2003, Office 2003, Windows Server 2003, IE 6

Windows users are advised to install the patch for a security loophole that could allow graphics to be vectors of malicious code. Those who have already installed XP S2 "should not be complacent." For details, see the *BBC News* report, "Image flaw exposes Windows PCs" at
http://news.bbc.co.uk/1/hi/technology/3661678.stm

NPR Reports on Wireless Insecurity

For some interesting insights into the privacy pitfalls of wireless, tune in to NPR's September 17 broadcast, "Wireless Internet Keeps Stat Fans Happy at Ballparks" at
http://www.npr.org/features/feature.php?wfId=3924653

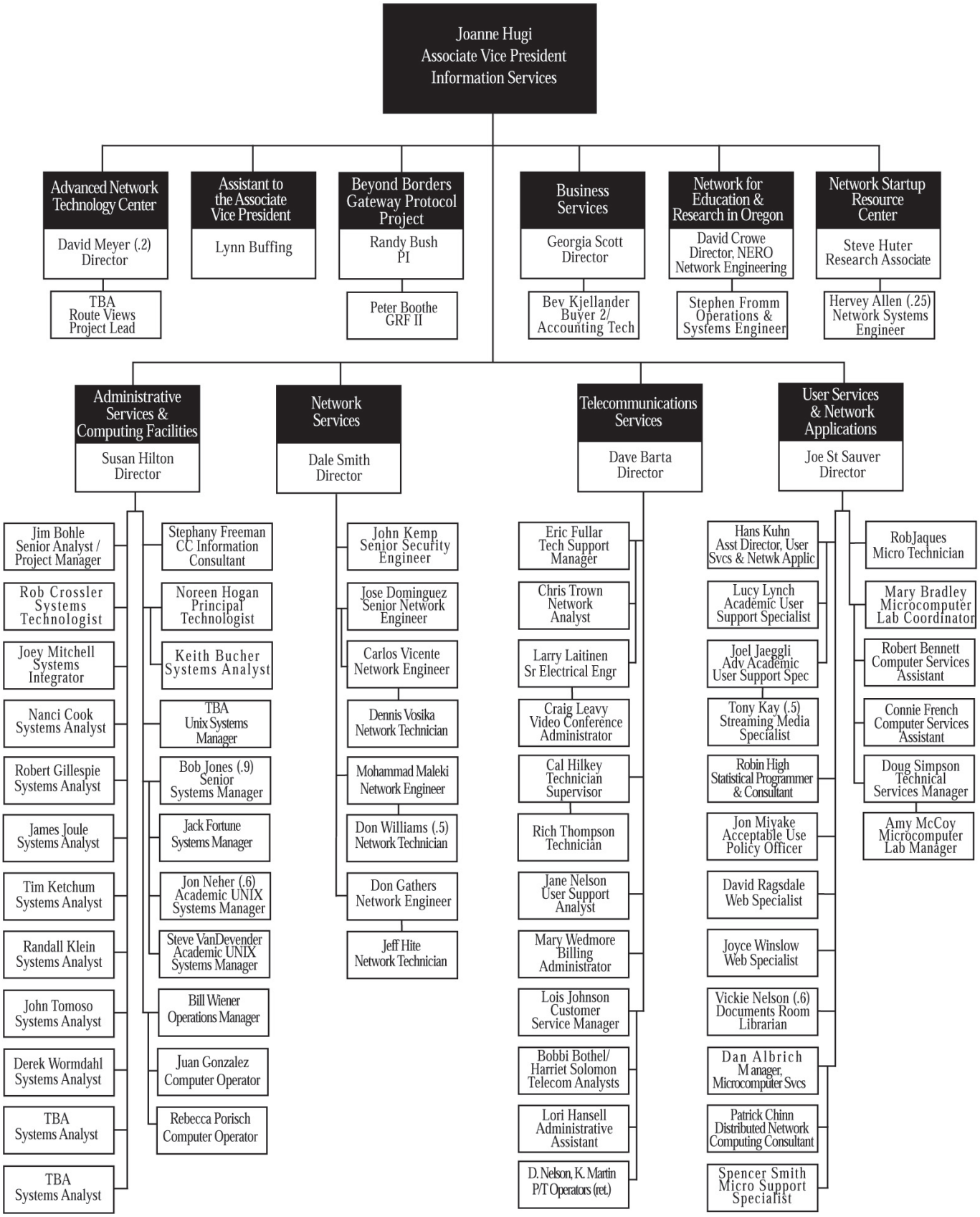
Beware 'Click to Remove' Instructions

Don't press any 'click to remove' links included with a spam message because they could trigger malicious code to run on vulnerable PCs. For details, go to
http://www.theregister.co.uk/2004/09/22/opt-out_exploit/

Older Windows Versions Denied Free IE Security Update

Microsoft's recent security improvements to IE are available only to XP users. If you run an earlier version of Windows, you'll have to pay to upgrade. See
http://news.com.com/Microsoft+to+secure+IE+for+XP+only/2100-1032_3-5378366.html

UO Computing Center Organization Chart
September 2004



COMPUTING CENTER GUIDE

UO Website
http://www.uoregon.edu/

Computing Center Website
http://cc.uoregon.edu/

Microcomputer Services
http://micro.uoregon.edu/

(151 McKenzie Hall)

- microcomputer technical support
- help with computing accounts, passwords
- scanning, CD burning, digital video
- help with damaged disks, files
- system software help
- Internet connections, file transfers
- public domain software, virus protection
- software repair (carry-in only, $80/hour, 1/2 hour minimum)

346-4412
microhelp@lists.uoregon.edu

Documents Room Library
http://darkwing.uoregon.edu/~docsrm/

(175 McKenzie Hall)
346-4406

Modem Number
Dialin modem number for UOnet, the campus network: **225-2200**

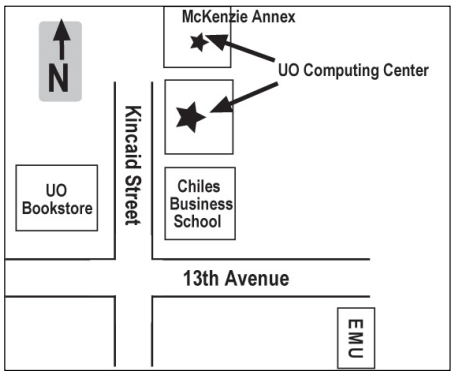
Large Systems Consulting
http://cc.uoregon.edu/unixvmsconsulting.html

(225-239 Computing Center)

- VMS, Unix
 (Gladstone, Darkwing, Oregon)
- email, multimedia delivery
- scientific and cgi programming
- web page development

346-1758
consult@darkwing.uoregon.edu
consult@gladstone.uoregon.edu

Statistics Consulting
Robin High
219 Computing Center
346-1718
robinh@uoregon.edu



Electronics Shop (151 McKenzie Hall)
http://cc.uoregon.edu/e_shop.html

Computer hardware repair, installation, and upgrades.
346-3548
hardwarehelp@oregon.uoregon.edu

Network Services
http://ns.uoregon.edu/

Provides central data communication and networking services to the UO community.
346-4395
nethelp@ns.uoregon.edu

Administrative Services
http://ccadmin.uoregon.edu/

Provides programming support for campus administrative computing, including BANNER, A/R, FIS, HRIS, and SIS. Call **346-1725**.

Computing Center Hours
Mon - Fri 7:30 A.M. - 5:00 P.M.

McKenzie Building Hours

Mon - Thu	7:30 A.M. - 11:30 P.M.
Friday	7:30 A.M. - 7:30 P.M.
Saturday	9 A.M. - 9:30 P.M.
Sunday	9 A.M. - 9:30 P.M.

- Note: These are *building* access hours; hours for individual facilities may vary.

O | UNIVERSITY OF OREGON
UO COMPUTING CENTER
1212 University of Oregon Eugene, OR 97403-1212